# DONNÉES DE LA RECHERCHE
## PROTECTION DES DONNÉES PERSONNELLES

**Patrick Guillot**
**Délégué à la protection des données (DPO) mutualisé**
**DPO@grenet.fr**

**11 décembre 2018**

Délégué à la protection des données

# préliminaires

?

- **Qu'est-ce qu'une donnée à caractère personnel ?**
- **quand a été créée la CNIL ?**
- **quelles sont les démarches à entreprendre pour être conforme à la loi ?**
- **le DPO c'est quoi ?**
- **…**

**VRAI/FAUX ?**

- **l'@IP de mon ordinateur est une donnée personnelle**
- **un questionnaire sans «données nominatives» est «anonyme»**
- **les colloques, conférences, etc. sont des traitements de données personnelles**
- **la législation sur les données personnelles est harmonisée au plan mondial**
- **….**

# vrai / faux (1)

| | |
|---|---|
| **L'adresse de messagerie professionnelle (institutionnelle) est une donnée à caractère personnel** | VRAI<br>au même titre que l'adresse de messagerie privée |
| **La redirection de la messagerie professionnelle sur la messagerie privée est tolérée** | FAUX<br>La sécurité des informations sensibles ou confidentielles n'est pas garantie |
| **Le N+1 peut accéder (consulter) la messagerie ou l'espace professionnels d'un personnel** | VRAI (les données sont réputées professionnelles)<br>en ayant informé la personne<br>FAUX pour les informations privées<br>conservées dans un répertoire clairement identifié «privé » |
| **Le mail n'est pas un moyen de communication sécurisé** | VRAI<br>équivaut à la carte postale pour le corps du message<br>A MINIMA : CHIFFRER LES PIECES JOINTES CONFIDENTIELLES ou SENSIBLES |
| **Traiter des données sensibles doit être autorisé par la CNIL** | VRAI<br>ces traitements sont a priori interdits |
| **L'annuaire interne des membres d'un laboratoire peut être publié sur le net** | FAUX<br>non conforme sans le consentement des personnes<br>admis sur intranet (intérêt légitime) |
| **Le.la doctorant.e est responsable des traitements de données personnelles utilisées pour son travail de thèse** | FAUX<br>la responsabilité juridique porte sur le laboratoire (UMR) ou l'établissement<br>le directeur de thèse est responsable de mise en œuvre |

# vrai / faux (2)

| | |
|---|---|
| La voix est une donnée personnelle<br>est une donnée personnelle biométrique | VRAI c'est bien une donnée personnelle<br>FAUX elle peut être déformée ou contrefaite |
| un questionnaire sans «données nominatives» est «anonyme» | FAUX<br>beaucoup d'autres informations permettent d'identifier une personne |
| les colloques, conférences, etc. sont des traitements de données personnelles | VRAI<br>on gère des listes de contacts, de participants, d'intervenants, la restauration, l'hébergement, etc. |
| Les recherches en santé sont soumises à des obligations spécifiques | VRAI<br>relèvent d'un chapitre particulier de la loi informatique et libertés et du Code de la santé publique |
| Ne pas s'opposer vaut consentement | FAUX<br>le consentement est un acte volontaire marqué, libre et éclairé.<br>Toute autre attitude vaut opposition |
| Le transfert (la communication) de données personnelles hors de l'Union européenne (UE) n'est pas autorisé | VRAI<br>l'UE est un périmètre de confiance pour la sécurité des données<br>le transfert hors UE est a priori interdit sauf autorisation de la CNIL |
| Les données « sociodémographiques » servant à la sélection et l'inclusion de personnes pour participer à des recherches sont des données à considérer (loi) | VRAI<br>Même si ces données n'interviennent pas directement dans le protocole, ce sont des données de recherche à caractère personnel dont le traitement est soumis aux obligations légales |

# LA PROTECTION DES DONNÉES PERSONNELLES EN RECHERCHE

## Loi informatique et libertés
## Règlement général européen sur la protection des données (RGPD)

Délégué à la protection des données

# Donnée(s) à caractère personnel (dcp) – fichier

- **Donnée à caractère personnel = toute information relative à une personne physique permettant de l'identifier…**
  - directement : nom et prénom, date de naissance, numéro d'identification (INSEE , N° étudiant, …), image (photo, vidéo, …), éléments biométriques (empreinte digitale, ADN...)…
  - ou indirectement : adresse (postale, mail), @IP, téléphone, biens (voiture, ordinateur, …), situation professionnelle, comportement, …
- **Données sensibles = les origines raciales ou ethniques ; les opinions politiques, philosophiques ou religieuses ; l'appartenance syndicale, relatives à la santé, à la vie sexuelle ; aux difficultés sociales, aux infractions ou condamnations ; données biométriques et génétiques**

  **+ le NIR** (n° INSEE ou n° sécurité sociale)
- **Fichier = ensemble de données à caractère personnel structurées, stables, accessibles et indépendantes du support**

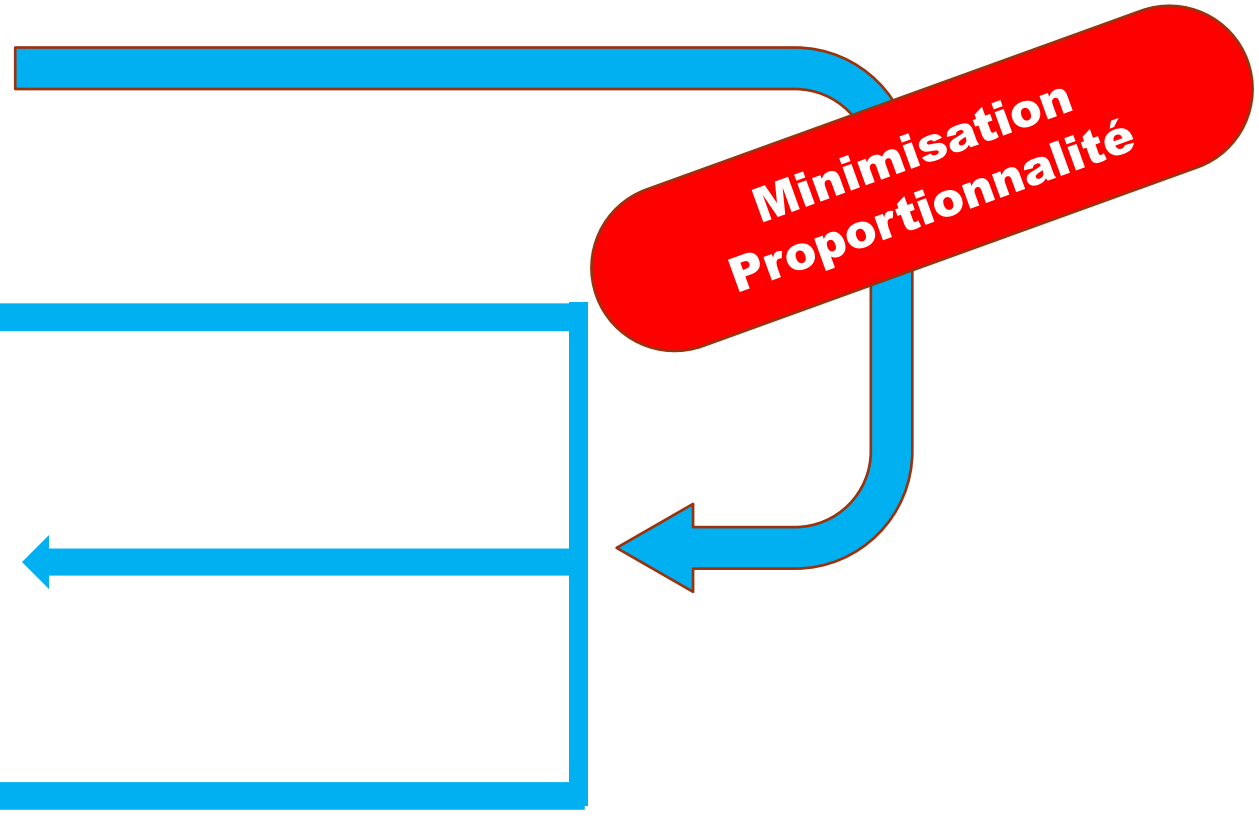
**dans le contexte privé ou professionnel**

# Traitement de données à caractère personnel

- **traitement : toute opération sur des dcp**
  - collecte, consultation, conservation, modification, diffusion, interconnexion … destruction
- **interdit, sauf exceptions et sur autorisation de la CNIL**
  - traitement de **données sensibles**
  - **interconnexion** (« croisement ») de fichiers dont les finalités sont différentes
  - transmission de DCP **hors Union Européenne**
- **conformité d'un traitement de données personnelles**
  - défini et mis en œuvre pour une **finalité déterminée et explicite**
  - soumis au **consentement libre et éclairé** des personnes concernées
  - selon une **information préalable sincère et compréhensible**
  - **collecte** et traite des **données pertinentes** et **non excessives**
  - garantit une **conservation des données** (hébergement , stockage) **limitée et sécurisée** (accès et **confidentialité**)
  - garantit l'**exercice des droits** des personnes concernées (accès, suppression…)
- **nb : traitement de données pour les projets de recherche portant sur des personnes**
  - **les protocoles de sélection et d'inclusion des personnes font partie du traitement des données**

# principes fondamentaux de la protection des données

- **Finalité du traitement**
  - déterminée, licite, loyale, légitime, explicite
- **Pertinence des données**
  - nécessaires à la finalité et non excessives
- **Conservation limitée des données**
  - pas plus que le temps nécessaire à leur utilité
- **Obligation de sécurité**
  - protection de bout en bout et par défaut
- **Information des personnes et respect de leurs droits**



# Les acteurs d'un traitement de données (1)

- **La loi protège (la vie privée de) toutes les personnes physiques partout**
  - **dans le contexte professionnel comme dans le contexte privé**
- **Les obligations portent sur tout organisme privé ou public**
  - **les secteurs enseignement et recherche sont soumis à la loi**
- **Responsable des traitements : la personne physique ou morale qui définit la finalité, les moyens et les conditions de mise en œuvre des traitements**
  - enseignement supérieur = EESR (université…) ou **UMR (recherche)**
  - responsabilité juridique portée par le chef d'établissement ou le/la directeur/trice du laboratoire
- **Sous-traitant : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement**
- **Responsable de mise en œuvre* : décideur fonctionnel ou opérationnel ou hiérarchique**
  - ex. recherche : directeur/trice de thèse
  - **ne peut être un étudiant ou doctorant**

*(*) fonction non définie par la loi*

# RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES (RGPD)
# GLOBAL DATA PROTECTION REGULATION (GDPR)

**Protection**

**→ confirmation et renforcement des droits des personnes**

**Obligations légales**

**→ responsabilité et preuves de conformité (documentation)**

# Historique des principaux textes

- **1978 : Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés**
- **1995 : Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données**
- **2004 : Loi n°2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés**
- **2012 : («loi Jardé») - Loi n° 2012-300 du 5 mars 2012 relative aux recherches impliquant la personne humaine**
- **2016 : (publication du RGPD) - Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données**
- **2016 : («loi Lemaire») - Loi n°2016-1321 du 7 octobre 2016 pour une République numérique (**
  - préfigure le RGPD : notamment ouverture des données publiques (open data) et de la recherche (science ouverte)
- **2017 : (Code de santé publique) - Décret n° 2017-884 du 9 mai 2017 modifiant certaines dispositions réglementaires relatives aux recherches impliquant la personne humaine**
- **2018 : 25 mai application du RGPD immédiate et uniforme dans tous les pays de l'UE**
  - **s'impose aux lois nationales**
- **2018 : Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles**
  - **transpose le RGPD dans la loi française**
  - **les recherches en santé et les traitements relevant des intérêts de l'Etat relèvent de la loi française**

# S’adapter aux nouveaux enjeux

- **Le développement des procédures dématérialisées**
  - services aux usagers (téléservices, …)
  - procédures internes (missions, …)
  - …
- **La mise à disposition des données**
  - cf. RGPD, Loi pour une république numérique
  - Open Data : libre accès aux données publiques administratives
  - Open science : réutilisation des données de la recherche publique
  - dans le respect de la vie privée des personnes concernées
- **Les nouvelles technologies**
  - plates-formes de formation, pédagogie inversée, …
  - objets connectés, …
- **Big data : collectes massives de données**
  - LPNR : incitation aux traitements de données en masse
  - RGPD : cadre protecteur pour la vie privée
- **Etc.**

# Objectifs du RGPD

- **Harmonisation du droit dans l'UE**
  - application du RGPD sans retranscription dans le droit national
  - uniformité du droit protecteur de la vie privée sur le territoire de l'UE
  - mise en place de Délégué.e.s à la protection des données (DPO)
- **Renforcement et extension des droits des personnes**
  - information, accès, droit à l'oubli, portabilité des données, …
  - **obtenir la preuve de la conformité du traitement de ses données (inversion de la charge de la preuve)**
- **Crédibilisation de la régulation européenne**
  - harmonisation européenne de la régulation et renforcement des sanctions
- **Ouverture et circulation des données**
  - **ouverture des données publiques (« Open data », « Open science »)**
- **Responsabilisation renforcée pour les responsables de traitement et les sous-traitants**
  - **Délégué à la protection des données (DPO) obligatoire dans le secteur public**
  - **documentation et preuves de la conformité continue**

# enjeux : impacts sur la vie privée

## I. la collecte des données

- les données d'inclusion/exclusion sont à prendre en compte
  - ce sont les **premières données collectée**s
  - ce sont **parfois** (souvent) **des données sensibles** (au sens de la loi)
  - ce sont des éléments de **l'analyse des risques et impacts** sur la vie privée
- impacts selon le type de données collectées (**pertinence**)
  - objectives ; confidentielles et/ou touchant à la vie privée ; sensibles
- impacts selon le volume de la collecte
  - nombre de personnes concernées ; nombre d'informations / personne
- impacts selon la source d'information
  - **la personne** ; un tiers ; fichier(s) constitué(s) ; **réseaux sociaux** ; etc.
- impacts selon le protocole et les outils de collecte
  - enregistrement : interview, vidéo, capteurs, …
  - questionnaires : papier, en ligne (**attention aux plates-formes dans le « cloud »**)
  - communication, extraction, requête sur un fichier
  - **par «moissonnage» (collecte massive, Big data)**

# enjeux : impacts sur la vie privée

## II. impacts selon la sécurité portée au données durant leur durée de conservation

- risques : fuite de données, accès illégitime, modification, suppression non souhaitée ; …
- **analyse des risques**
  - maîtrise depuis la collecte à la publication des résultats (et à la suppression des données brutes)

## III. impacts selon la possibilité d'identifier des personnes… Vous avez dit anonymat ?

- **différencier confidentialité et anonymat**
- les données brutes sont (toujours) des données personnelles
- l'anonymat strict n'existe (quasiment) pas !
- **des «données non nominatives» ne sont pas anonymes**
- recommandation systématique : «***pseudonymisation***»
  - **minimisation** du caractère identificateur (indirect) des données

## IV. impacts selon la mise à disposition des données (destinataires)

- accès public aux résultats : données de publication (agrégées)
- ouverture des données de recherche (**open access**) ; recherche ouverte (**open rech**erche)
  - aux publics scientifiques
  - obligation de la loi pour une république numérique si financement public
  - les données brutes doivent être ***pseudonymisées***
- **nb : toute réutilisation de données constitue un nouveau traitement soumis aux dispositions légales**

# Évolution des obligations : droits des personnes confirmés et étendus

- **Information préalable explicite, transparente et complète (art. 13-14)**
  - au plus tard à la collecte des données
- **Consentement libre et éclairé (art. 7)**
  - **Nb : la charge de la preuve incombe au RT**
- **Droit de demander la limitation du traitement (art. 18)**
  - ex. profilage, données excessives, …
- **Droit d'accès facilité (art. 15)**
- **Droit à la portabilité des données (art. 20)**
- **Droit à l'oubli (art. 17)**
- **Droit à notification de violations de ses données (art. 34)**
- **Droit de ne pas faire l'objet d'une décision automatisée (art. 22)**
  - ex. profilage, sélection automatique d'étudiants (ex. APB),
- **Droit de donner des directives pour le sort de ses données post mortem**
- **Réparation des préjudices (art. 82)**

# Évolution des obligations : nouveaux principes

- **Accountability : responsabilité et de preuve de conformité**
  - **le directeur/trice de l'unité où est menée la recherche est responsable de traitement**
  - **le/la responsable scientifique est responsable de mise en œuvre**
  - **documentation : consentement, protocole, analyse de risque, cahier de labo, autorisation CNIL, …**
  - **en cas de sous-traitance : contrat**
- **Privacy by design : prise en compte des aspects informatique et libertés et des impacts dès le début du projet (cahier des charges)**
  - **principe de minimisation** selon le protocole de la recherche : **pertinence** des données, **durées de conservation**
  - maîtrise des données : **localisation** et **sécurité** à porter aux données
  - **information** complète, loyale, explicite **et consentement éclairé**
- **Privacy by default : protection par défaut**
  - mesures techniques **et** organisationnelles (sécurité et confidentialité)
    - sur les outils : infra, applications, anonymisation, chiffrement…
    - sur les processus : méthodes, protocoles, habilitations…
- **Privacy impact assessment (PIA) ou étude d'impact sur la vie privée (EIVP)**
  - analyse de risques spécifique avec le Délégué à la protection des données (DPO)
  - détermine la nécessité de soumission préalable à la CNIL.

# SE PRÉPARER AU RGPD...

**en pratique, on fait quoi ?**

Délégué à la protection des données

# Les questions à se poser

| | |
|---|---|
| Ai-je le droit de traiter ces données ? (licéité) | En recherche, c'est le consentement de la personne concernée qui fonde la licéité |
| Pourquoi ? (finalités) | L'objectif de la recherche est décrit de manière explicite |
| Sur qui ? (personnes concernées) | Toutes les personnes dont les données personnelles peuvent être traitées (utilisées) |
| Quoi ? (données) | Veiller à la pertinence des données collectées et traitées (ex. date de naissance |
| Où ? (lieu de conservation) | Où sont stockées les données tout au long de la recherche ? Attention aux serveurs « cloud » |
| Jusqu'à quand ? (durée de conservation) | Veiller à supprimer dès que possible les données identifiant des personnes |
| À qui ? (destinataires des données) | Quelles sont les personnes pouvant accéder aux données ? (autres chercheurs…)<br>Quelles données seront mise à disposition en « open research » ? |
| Comment ? Quelle sécurité ? | Décrire les processus de mise en œuvre de la recherche<br>Décrire les moyens de mise en œuvre et la sécurité |
| Le traitement est-il « à risque » ? | Évaluer le niveau d'impact(s) sur la vie privée des personnes concernées |
| Quelles preuves de « conformité RGPD »? | Documenter l'ensemble des activités du traitement depuis la sélection et l'inclusion, l'information et le recueil du consentement, jusqu'à la publication des résultats et la mise à disposition éventuelle des données |
| Quelles sont les responsabilités ? | Le/la directeur/trice des unités multi-tutelles est responsable de traitement<br>Le responsable scientifique de la recherche est responsable de la mise en œuvre |

# Mesures de conformité pour les personnes traitant des données de recherche

| Portée des mesures | Mesures, bonnes pratiques |
|---|---|
| • Hébergement des données | Maîtrise et sécurisation<br>Pas de cloud public (limesurvey, monkeysurvey, google drive/doc/form…) |
| • Conservation des données | Archivage : dans quel but et combien de temps ?<br>Pas de conservation illimitée sur l'ordinateur |
| • Transfert des données | Pas par mail<br>Pas de we transfer<br>Dépôt sur des espaces sécurisés (ex. FileSender) |
| • Proportionnalité des données | Se poser la question de la nécessité de collecter telle ou telle donnée |
| • Confidentialité des données | Sécuriser les accès et limiter les destinataires aux seules personnes légitimes<br>Chiffrement des données confidentielles ou sensibles |
| • Archivage des données | Publications… |

# RECHERCHES TRAITANT DES DONNÉES PARTICULIÈRES

## recherches impliquant la personne humaine (RIPH)
## recherches en santé

# Recherches impliquant la personne humaine (RIPH)

## Les RIPH sont définies par le Code de la santé publique (art. L1121-1)

- Type 1 : "Les recherches interventionnelles qui comportent une intervention sur la personne non justifiée par sa prise en charge habituelle"
- Type 2 : "Les recherches interventionnelles qui ne comportent que des risques et des contraintes minimes, dont la liste est fixée par arrêté du ministre chargé de la santé, après avis du directeur général de l'Agence nationale de sécurité du médicament et des produits de santé"
- Type 3 : " Les recherches non interventionnelles qui ne comportent aucun risque ni contrainte dans lesquelles tous les actes sont pratiqués et les produits utilisés de manière habituelle"
  - **ex. thèses / études de médecine générale par questionnaires, interviews**

## Cadre réglementaire

- la loi du 5 mars 2012 modifiée (loi Jardé)
- Code de la santé publique
- Encadrement éthique
  - soumission du dossier au **Comité d'éthique pour les recherches** (CER Grenoble Alpes)
  - et/ou soumission du dossier au **Comité de protection des personnes** (CPP)
- RGPD et loi informatique et libertés

# Recherches en santé : bases juridiques (licéité)

- **Selon le cas**

1. **engagement de conformité à une méthodologie de référence : MR-00x**
2. **sinon**
    1. **recherches impliquant la personne humaine**
        1. demande d'autorisation à la CNIL
    2. **recherches n'impliquant pas la personne humaine**
        1. ex. recherches rétrospectives (données de santé collectées indirectement)
        2. dossier soumis à l'Institut national des données de santé (INDS) qui transmet à la CNIL

# Conformité des recherches (surtout SHS et santé)

## Principe de minimisation

- pseudonymisation des données (open science)

## Sécurité et confidentialité

- **chiffrement des ordinateurs portables** où sont conservés les fichiers de données de recherche (recommandation PSSI)
- **a minima** : **chiffrement des fichiers** contenant les données

## Évaluation des impacts sur la vie privée (EIVP)

- envisager une EIVP si les **risques sur la vie privé**e sont importants
- avec **au minimum le responsable scientifique et le DPO**

## Formalités et accompagnement

- soumettre les projets SHS au **comité d'éthique pour les recherches** (CER Grenoble Alpes)
- documenter les activités du traitement (dossier descriptif du projet)
- **rencontrer le DPO** le plus tôt possible (toujours nécessaire une 1ère fois au moins avec le/la responsable scientifique)
- Difficulté : **disponibilité des ressources d'accompagnement**

# MERCI DE VOTRE ATTENTION

**Questions ?**

Délégué à la protection des données